

STATE OF NORTH CAROLINA
COUNTY OF WAKE

**Memorandum of Understanding
Information Security Threat Responsibilities**

The purpose of this Memorandum of Understanding is to define the roles and responsibilities of State agencies when faced with a security threat to the State's information assets. Appropriate, legal, and complete information protection mechanisms must be executed in response to a threat to the State's information assets. Herein, the State Chief Information Officer, the Office of Information Technology Services, the Office of State Auditor and the Department of Justice (hereinafter, the Agencies) agree on the appropriate response to threats identified by Information Technology Services. On December 14, 1998 and January 28, 2002, the Agencies executed Memoranda of Understanding concerning their responsibilities for response to information security threats. Due to additional statutory duties and the State's response to terrorism, those MOUs are hereby superseded.

N.C.G.S. §114-15.1 requires that the State Bureau of Investigation receive written notification of any information or evidence of "damage of, theft from, or theft of, ... or misuse of, any State-owned personal property...." This reporting requirement includes reports of a security threat or breach of the State's information systems. N.C.G.S. §147-64.6(c)(16) states that the Office of the State Auditor is responsible for receiving reports of improper governmental activities, including any misappropriation of State resources or any violation of State or federal law, rule or regulation. N.C.G.S. §147-64.6(c)(12) requires the State Auditor to provide a written report of "... apparent violations of penal statutes or apparent instances of malfeasance, misfeasance or nonfeasance by an officer or employee" to the Governor and Attorney General, and other appropriate officials. N.C.G.S. §147-64.6(c)(18) requires the State Auditor, after consultation and in coordination with the State Chief Information Officer (State CIO), to assess, confirm, and report on the security practices of information technology systems.

N.C.G.S. §§147-33.82(a)(4) and 147-33.110 require the State CIO to establish statewide standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets. The legislative and judicial branches, the University of North Carolina and its constituent institutions, local school administrative units, and the Community Colleges System shall adopt security standards that are comparable to or exceed those set by the State CIO. N.C.G.S. §147-33.111(b). The State CIO may assume the information technology security function of any State agency that fails to adhere to security standards adopted pursuant to N.C.G.S. §147-33.110, and report such action to the Information Technology Advisory Board at its next scheduled meeting. N.C.G.S. §147-33.113(a)(1) requires State agencies to report their information technology security incidents to the State CIO within 24 hours of confirmation.

The Agencies' concerted efforts to react to any perceived threat to the State's information assets in a well defined, efficient and effective response is, in itself, a major deterrent to unacceptable behaviors.

The roles and responsibilities of the Agencies charged by law with protecting the State's information assets are summarized below.

The Office of Information Technology Services (ITS) is part of the Office of the Governor under the direction of the State CIO. At the direction of the State CIO, ITS must take appropriate steps to protect the State's information assets within its control and to establish statewide information technology security standards.

The roles and responsibilities of the State CIO and ITS in establishing information security standards and in response to a breach of security consist of, but are not limited to, the development and implementation of policies and procedures to:

- Establish an enterprise-wide set of policies and standards for information technology security of the State's distributed information technology assets and to annually review those standards.
- Periodically review the existing security standards and practices in place among the various State agencies.
- Coordinate and consult with the Office of State Auditor as the Auditor assesses confirms, and reports on the security practices of information technology systems in state government.
- Detect security threats and breaches.
- Investigate to determine the source and nature of security threats and breaches.
- Mitigate the adverse effects of security threats and breaches.
- When and if necessary, terminate access to the network from the area of the breach, until the security breach is identified and contained.
- Possibly assume the information technology security function of any State agency that fails to adhere to required security standards.
- Record, classify, track and report security threats.
- Assess the risk associated with each type of threat.
- Define appropriate threat responses using specialized security response teams.
- Notify the agency or agencies that could possibly be impacted by identified security threats and breaches.
- Notify the State Bureau of Investigation and the Office of the State Auditor in a mutually acceptable written format and within a mutually acceptable timeframe of any security threats and breaches that meet predetermined severity criteria.
- Support the efforts of State agencies to respond to threats and security breaches.
- Document policies and procedures for threat response.
- Maintain a program designed to mitigate risk or completely eliminate risk from previously identified threats.
- Assess the ability of each agency to comply with the current security enterprise-wide set of standards and to assess each agency's security organization, network security architecture, and current expenditures for information technology security.

(Please refer to the ITS Information Security Incident Reporting Procedures, <https://incident.its.state.nc.us/>)

The Office of the State Auditor (OSA), under the leadership of the State Auditor, provides the citizens of North Carolina with professional, independent evaluations of the State's fiscal accountability and public program performance. It is charged with assessing, confirming, and reporting on the security practices of information technology systems.

The roles and responsibilities for OSA in response to security breaches reported by ITS consist of, but are not limited to, the development and implementation of policies and procedures to:

- Identify appropriate controls for managing information security threats and breaches.
- Conduct network penetration testing or similar procedures as deemed necessary by OSA.
- Investigate reported information technology security breaches, cyber attacks, and cyber fraud in State government.
- Audit agency procedures and operations for responding to security threats and breaches.
- Audit agency procedures and operations for recording and tracking security threats from inception to closure.
- Audit agency procedures and operations to ensure that each type of reported threat is properly classified.
- Audit agency procedures and operations to ensure that risks associated with each type of reported threat are properly evaluated and assessed
- Evaluate the adequacy of agency information security threat responses.
- Work with the State CIO, ITS, the Attorney General, and the State Bureau of Investigation to establish mutually acceptable standards and controls for written information exchange of identified security threats and breaches.
- Support the efforts of the State CIO and State agencies to respond to threats and security breaches.
- Document the audit results and suggest improvements for agency information threat responses.
- Maintain an archive of documented audit results for the legally required timeframe.

The North Carolina Department of Justice is under the direction of the Attorney General. This department is organized into two main responsibility areas relating to this Memorandum of Understanding: law enforcement and legal services.

The North Carolina State Bureau of Investigation (SBI) is a part of the Department of Justice under the direction of the Director of the SBI. It investigates criminal activities and works for a more effective administration of the criminal laws of the State.

The roles and responsibilities of the SBI in preparation for and in response to a possible criminal breach of information security reported by ITS include, but are not limited to, the development of policies and implementation of procedures to:

- Review and make recommendations as to the State's information security standards.
- Determine if reported security breaches include possible criminal activities.

- Investigate suspected criminal activities related to information security threats and breaches when appropriate.
- Support the efforts of State agencies to respond to threats and security breaches.
- Document policies and procedures for threat response.
- Maintain an archive of documented investigative findings.

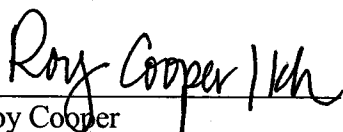
The North Carolina Office of the Attorney General provides legal representation to State departments, agencies and commissions as required by law.

The roles and responsibilities of the Attorney General in response to a reported breach of information security consist of, but are not limited to, the development and implementation of policies and procedures to:

- At an agency's request, determine possible legal liabilities and potential legal actions that might result from reported security breaches.

As a representative of my agency, I acknowledge that I have read this document and agree that my agency will comply with this Memorandum of Understanding for Information Security Threat Responsibilities. I agree to inform the appropriate staff at my agency of the need to respond to information security threats and breaches in the manner described in this memorandum.

This agreement takes effect immediately after all parties have signed it. All parties to this agreement must mutually agree in writing to any changes. This agreement remains in effect until any agency participant provides written notification to all the other parties to this agreement of their intention to terminate this memorandum of understanding. Any written notification of termination of this memorandum of understanding must include a termination date that provides at least two weeks' advance notification to all parties. OSA, DOJ and the State CIO have executed duplicate originals of this Memorandum of Understanding on this, the ___ day of April, 2006.



Roy Cooper
Attorney General
N.C. Department of Justice



Leslie W. Merritt, Jr.
State Auditor
N.C. Office of State Auditor



George Bakolia
State Chief Information Officer
N.C. Office of Information Technology Services



Robin P. Pendergraft
Director
State Bureau of Investigation
N.C. Department of Justice

Received by ESRMD on 2-14-07